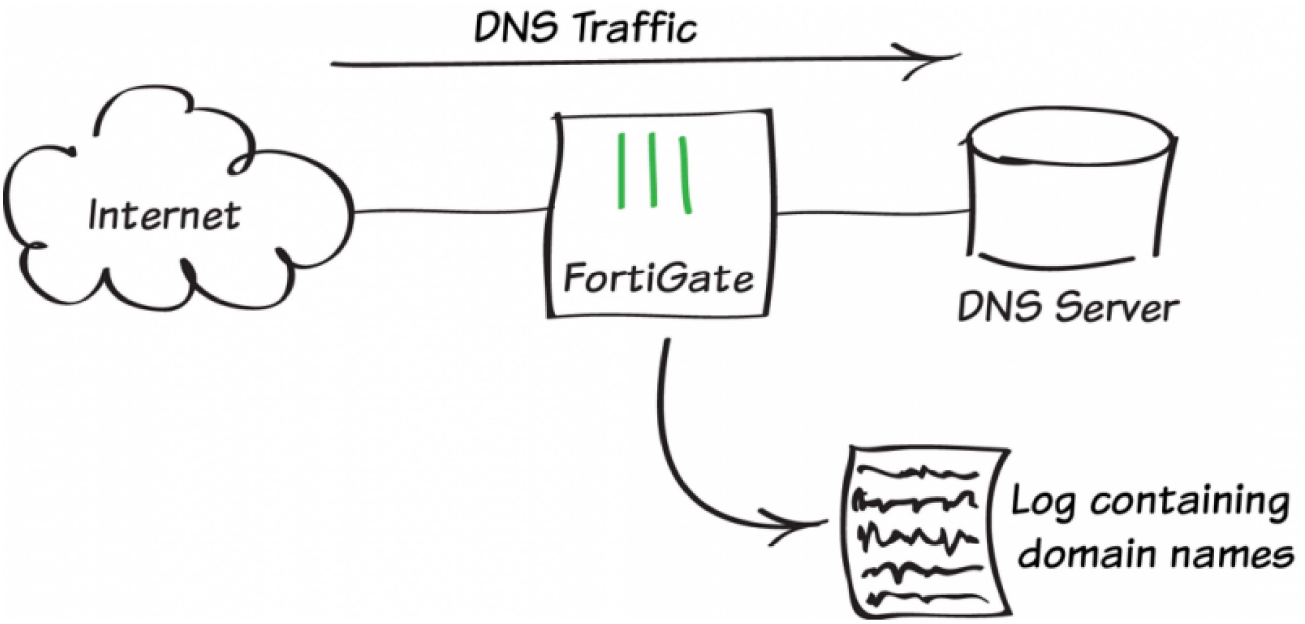
FORTINET

The FortiGate Cookbook

Recipes for success with your FortiGate

Logging DNS domain lookups

Posted on November 25, 2014 · 0 Comments

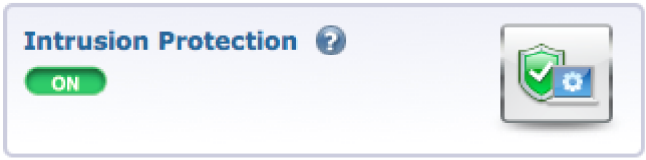


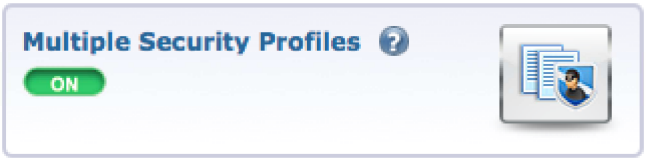
In this recipe, you will add a custom Intrusion Protection (IPS) signature to a security policy to record all domain lookups accepted by the policy. The signature records an IPS log message containing the domain name every time a DNS lookup occurs.

1. Enabling Intrusion Protection and multiple security profiles

Go to **System > Config > Features** and

enable **Intrusion Protection**. Select **Show More** and enable **Multiple security profiles.**



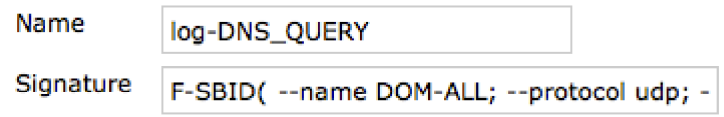


Apply the changes.

2. Creating a custom IPS signature

Go to **Security Profiles > Intrustion Protection** and select **View IPS Signatures**.

Create a new signature with this syntax. (You can copy and paste this text into the **Signature** field.)

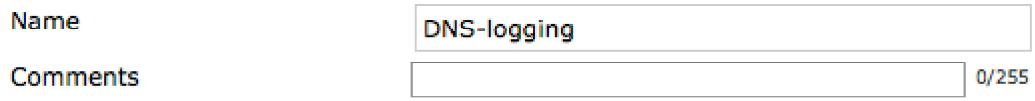



```
F-SBID( --name DOM-ALL; --protocol udp; --service dns; --log
DNS_QUERY;)
```

3. Adding the signature to an IPS profile

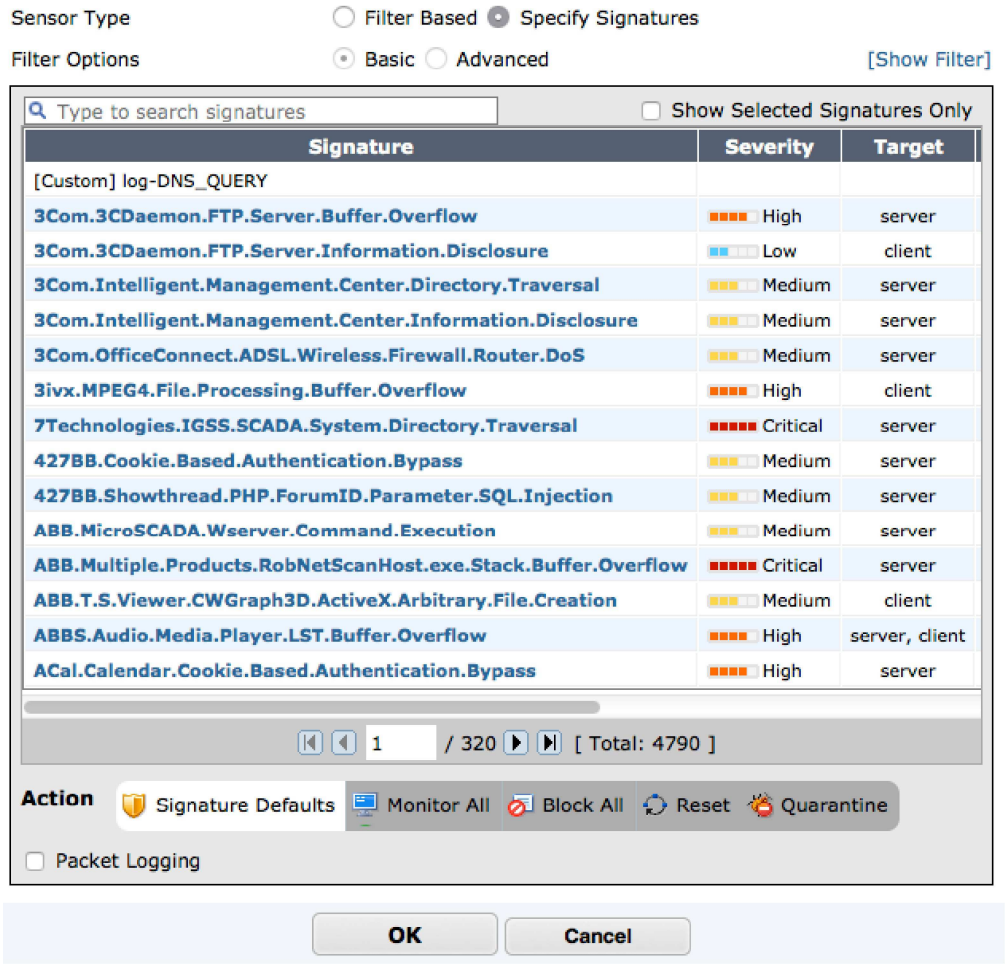
Go to **Security Profiles >**

Intrusion Protection and create a new profile.



Under **Pattern Based Signatures and Filters**, select **Create New**.

Set **Sensor Type** to Specify Signatures. The new signature should appear at the top of the list. If it does not, search for the signature's name (in the example, *log-DNS_QUERY*).



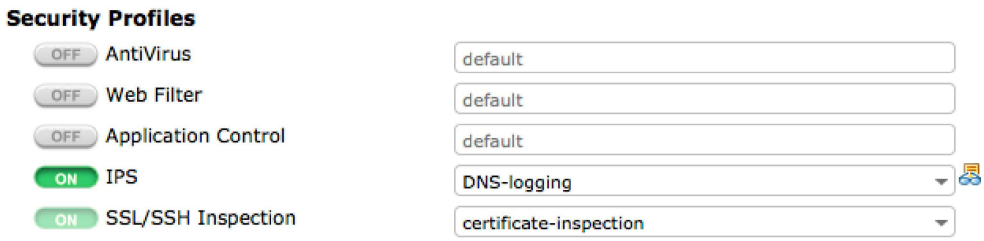
Select the signature, then select **OK**.

4. Adding the profile to the DNS server's security policy

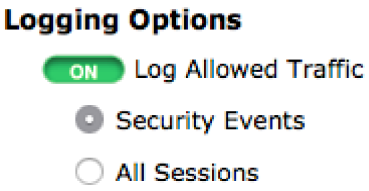
Go to **Policy & Objects > Policy >** IPv4 and edit the policy allowing

traffic to reach the DNS server.

Under **Security Profiles**, enable **IPS** and select the new profile.



Under **Logging Options**, enable **Log Allowed Traffic** and select **Security Events**.



5. Results

Go to **Log & Report > Security Log > Intrustion Protection.***

#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		07:51:31		192.168.200.110	udp		detected		DOM-ALL
2		07:51:32		192.168.200.110	udp		detected		DOM-ALL
3		07:51:32		192.168.200.110	udp		detected		DOM-ALL
4		07:51:31		192.168.200.110	udp		detected		DOM-ALL
5		07:51:32		192.168.200.110	udp		detected		DOM-ALL
6		07:51:31		192.168.200.110	udp		detected		DOM-ALL
7		07:51:31		192.168.200.110	udp		detected		DOM-ALL
8		07:51:32		192.168.200.110	udp		detected		DOM-ALL
9		07:51:32		192.168.200.110	udp		detected		DOM-ALL
10		07:51:31		192.168.200.110	udp		detected		DOM-ALL

You will see that the IPS profile has detected matching traffic.

If you select an entry, you

can view more information.

The domain name is shown in the **Message** field.

#	38	**Action**	detected
Attack ID	4153	**Attack Name**	**DOM-ALL**
Date/Time	07:51:29	**Destination**	192.168.110.9
Direction	0	**Dst Port**	53
Event Type	signature	**Incident Serial No.**	216891970
Level		**Log ID**	16384
Message	custom: DOM-ALL, dns_query=trello.com;	**Profile Name**	DNS-logging
Protocol	udp	**Protocol Number**	17

If you have a FortiAnalyzer, you can create a custom dataset for the DNS query by going to **Reports > Advanced > Dataset**.

Name: DNS-Query

Log Type: Attack

Query:

```
select msg, sum(totalnum) as totalnum from
###(select srcip, msg, count(*) as totalnum from
$log where $filter-exclude-var group by srcip,
msg order by totalnum desc)### t where $filter-
var-only and msg is not null group by msg order
by totalnum desc
```

This dataset can then be used in a custom report.

FORTINET

TOP 10 requested DNS Domains

#	Message	totalnum	% of Total
1	custom: DNS-A-Request, dns_query=init-p01st.push.apple.com;	57	3.68
2	custom: DNS-A-Request, dns_query=init-s01st.push.apple.com;	49	3.17
3	custom: DNS-A-Request, dns_query=www.google.com;	49	3.17
4	custom: DNS-A-Request, dns_query=www.apple.com;	44	2.84
5	custom: DNS-A-Request, dns_query=local;	40	2.58
6	custom: DNS-A-Request, dns_query=apple.com;	38	2.45
7	custom: DNS-A-Request, dns_query=p07-btmmdns.icloud.com;	34	2.20
8	custom: DNS-A-Request, dns_query=apple-mobile.query.yahooapis.com;	31	2.00
9	custom: DNS-A-Request, dns_query=dell.com;	30	1.94
10	custom: DNS-A-Request, dns_query=api.bing.com;	26	1.68
11	**Others**	**1150**	**74.29**
12	**Total**	**1548**	**100.00**

For further reading, check out DNS Service in the FortiOS 5.2 Handbook.

Related posts:

- Protecting a web server
- Logging FortiGate traffic
- Troubleshooting FortiGate logging

Posted in 5.2.0, 5.2.1, 5.2.2, FortiOS 5.2, Security Tagged DNS, IPS, logging

Powered by WordPress & Themegraphy